CONTRACTOR PROTECTION OF ELECTRONIC COUNTY INFORMATION

(BOARD OF SUPERVISORS POLICY NO. [TBD])

IMPLEMENTATION GUIDELINES

This document ("Guidelines") provides instructions on how to implement the Los Angeles County Board of Supervisors ("Board") Contractor Protection of Electronic County Information Policy (Policy No. **[TBD]**) ("Policy"), which was adopted by the Board on _____, 2016, and became effective _____ 2016. These Guidelines address the following areas:

- Introduction
- Implementation Oversight
- Department Assessment
- Notification of Contractors
- Standard Solicitation/Contract Language
- Questions

Introduction

The Board has recognized that the County of Los Angeles ("County") must ensure that appropriate safeguards are in place to protect public data and avoid the penalties and fines that may be imposed when unprotected confidential/sensitive information is disclosed inappropriately. The Policy was adopted to protect personal information ("PI"), protected health information ("PHI") and medical information ("MI") electronically stored and/or transmitted by County of Los Angeles Contractors ("Contractors").

Implementation Oversight

The Chief Executive Office ("CEO") shall provide overall oversight of the County's implementation efforts. Such oversight shall include compilation of a written report detailing the County's progress in implementing the Policy. The foregoing report shall be provided to the Board starting one hundred twenty (120) days after the adoption of the Policy by the Board, and every one hundred twenty (120) days thereafter, until the CEO verifies to the Board in writing that every Department has completed its implementation efforts. Thereafter, CEO shall provide the Board an annual report detailing the County's ongoing compliance efforts.

Department Assessment

Departments shall prioritize contracts for inclusion of the encryption requirements in accordance with the following risk-based criteria:

Each department will conduct a risk assessment of existing contracts to determine and establish a priority listing of all of their contracts that may require inclusion of contract language requiring contractors to implement encryption requirements.

In conducting the assessment, each department will utilize the following risk-based criteria:

(i) The type of County data being stored and/or transmitted by the contractor (i.e. PI, PHI, and/or MI);

(ii) The type and extent (e.g., continuous/occasional) of services critical to departmental business operations; and,

(iii) The highest contract value will be addressed working downward.

Each department will identify and evaluate all pending solicitations that may require inclusion of encryption language in accordance with the previously stated risk-based criteria.

Each department will identify and evaluate existing contracts as such contracts become due for amendment and/or renewal. While departments are not required to amend any contract solely to include these encryption requirements, in the case of contracts deemed to be especially high-risk, departments are advised to amend the contract as soon as reasonably practicable.

Each departmental information security officer (DISO) shall oversee implementation of the County's encryption requirements while coordinating with their respective contract management.

No less than once every thirty (30) days after adoption of the Policy by the Board, each Department shall submit a written report to CEO detailing its implementation efforts. The CEO may change the foregoing reporting requirements upon written notice to each Department.

Notification of Contractors

Each department will notify its Contractors of this Policy as appropriate.

DISOs shall provide minimum direction to Contractors without being prescriptive.

Validation

Each department will conduct an annual departmental validation using the previously stated risk-based criteria to identify contracts for the DISO to perform oversight and to validate the Contractor's performance. The DISO's oversight may consist of the following: (i) requiring the Contractor to certify its compliance with County's encryption policy; (ii) review of validation/attestation reports that Contractor's data encryption product(s) generate; and (iii) validation of other security and privacy measures to address logical, physical, and administrative measures.

Validation is done annually based on the results of the department's risk-based criteria review.

Departmental contract monitoring of this Policy will occur in accordance with the contract's audit or other related provisions.

Standard Solicitation/Contract Language

To fully implement the Policy, all County departments will be required to include appropriate language in their solicitations and contracts in accordance with the instructions set forth below:

1. Solicitations

All County solicitations must include standard language requiring proposers to certify that they maintain or will maintain certain encryption standards for the protection of electronic County PI, PHI and MI, when awarded a contract.

STANDARD LANGUAGE TO BE INCLUDED IN ALL SOLICITATIONS

Protection of Electronic County PI, PHI and MI – Data Encryption Standard

The prospective contract is subject to the encryption requirements set forth below (collectively, the "Encryption Standards"). Proposers shall become familiar with the Encryption Standards and the pertinent provisions of the Sample Contract, Appendix X, paragraph x.xx both of which are incorporated by reference into and made a part of this solicitation.

Proposers shall be required to complete Exhibit X in Appendix D – Required Forms ("Exhibit") providing information about their encryption practices and certifying that they will be in compliance with the Encryption Standards at the commencement of the contract and during the term of any contract that may be awarded pursuant to this solicitation. Proposers that fail to comply with the certification requirements of this provision will be considered non-responsive and excluded from further consideration.

Proposers use of remote servers (e.g. cloud storage, Software-as-a-Service or SaaS) for storage of County PI, PHI and/or MI shall be disclosed by Proposers in the Exhibit and shall be subject to written pre-approval by the County's Chief Executive Office. Any use of remote servers may subject the Proposer to additional encryption requirements for such remote servers.

Encryption Standards

Stored Data

Contractors' and subcontractors' workstations and portable devices (e.g., mobile, wearables, tablets, thumb drives, external hard drives) require encryption (i.e. software and/or hardware) in accordance with:

a) Federal Information Processing Standard Publication (FIPS) 140-2;
b) National Institute of Standards and Technology (NIST) Special Publication 800-57 Recommendation for Key Management – Part 1: General (Revision 3);
c) NIST Special Publication 800-57 Recommendation for Key Management – Part 2: Best Practices for Key Management Organization; and
d) NIST Special Publication 800-111 Guide to Storage Encryption Technologies for End User Devices.

Advanced Encryption Standard (AES) with cipher strength of 256-bit is minimally required.

Transmitted Data

All transmitted (e.g. network) County PI, PHI and/or MI require encryption in accordance with:

a) NIST Special Publication 800-52 Guidelines for the Selection and Use of Transport Layer Security Implementations; and
b) NIST Special Publication 800-57 Recommendation for Key Management – Part 3: Application-Specific Key Management Guidance.

Secure Sockets Layer (SSL) is minimally required with minimum cipher strength of 128-bit.

2. Contracts/Amendments

STANDARD LANGUAGE TO BE INCLUDED IN ALL CONTRACTS AND AMENDMENTS

XX. Data Encryption

Contractor and Subcontractors that electronically transmit or store personal information (PI), protected health information (PHI) and/or medical information (MI) shall comply with the encryption standards set forth below. PI is defined in California Civil Code Section 1798.29(g). PHI is defined in Health Insurance Portability and Accountability Act of 1996 (HIPAA), and implementing regulations. MI is defined in California Civil Code Section 56.05(j).

a. Stored Data

Contractors' and Subcontractors' workstations and portable devices (e.g., mobile, wearables, tablets, thumb drives, external hard drives) require encryption (i.e. software and/or hardware) in accordance with: (a) Federal Information Processing Standard Publication (FIPS) 140-2; (b) National Institute of Standards and Technology (NIST) Special Publication 800-57 Recommendation for Key Management – Part 1: General (Revision 3); (c) NIST Special Publication 800-57 Recommendation for Key Management – Part 2: Best Practices for Key Management Organization; and (d) NIST Special Publication 800-111 Guide to Storage Encryption Technologies for End User Devices. Advanced Encryption Standard (AES) with cipher strength of 256-bit is minimally required.

b. Transmitted Data

All transmitted (e.g. network) County PI, PHI and/or MI require encryption in accordance with: (a) NIST Special Publication 800-52 Guidelines for the Selection and Use of Transport Layer Security Implementations; and (b) NIST Special Publication 800-57 Recommendation for Key Management – Part 3: Application-Specific Key Management Guidance. Secure Sockets Layer (SSL) is minimally required with minimum cipher strength of 128-bit.

c. Certification

The County must receive within ten (10) business days of its request, a certification from Contractor (for itself and any Subcontractors) that certifies and validates compliance with the encryption standards set forth above. In addition, Contractor shall maintain a copy of any validation/attestation reports that its data encryption product(s) generate and such reports shall be subject to audit in accordance with the Contract. Failure on the part of the Contractor to comply with any of the provisions of this Sub-paragraph XX (Data Encryption) shall constitute a material breach of this Contract upon which the County may terminate or suspend this Contract.

Questions

Any questions regarding the foregoing Guidelines should be directed to the applicable DISO.